RENE L. VALLADARES
Federal Public Defender
State Bar No. 11479
SHARI L. KAUFMAN
Assistant Federal Public Defender
411 E. Bonneville, Ste. 250
Las Vegas, Nevada 89101
(702) 388-6577
(Fax) 388-6261

Counsel for ANDRE NESTOR

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

UNITED STATES OF AMERICA, Plaintiff, vs. ANDRE NESTOR, Defendant.	2:11-cr-00022-JCM-RJJ **MOTION TO DISMISS COUNT THREE OF THE INDICTMENT FOR FAILURE TO STATE AN OFFENSE AND VAGUENESS** **(Oral Argument Requested)**

COMES NOW the defendant, ANDRE NESTOR, by and through his counsel of record, Shari L. Kaufman, Assistant Federal Public Defender, and hereby moves this Court to enter an order dismissing Count Three of the Indictment. This Motion is supported by the attached Memorandum of Points and Authorities.

DATED this 9th day of November 2011.

RENE L. VALLADARES
Federal Public Defender

/s/ Shari L. Kaufman
By_____
SHARI L. KAUFMAN,
Assistant Federal Public Defender

MEMORANDUM OF POINTS AND AUTHORITIES

I.

STATEMENT OF FACTS

On January 19, 2011, the United States Attorney for the District of Nevada filed a three count indictment charging Andre Nestor ("Mr. Nestor") and co-defendant John Kane ("Mr. Kane") with one count of Conspiracy to Commit Wire Fraud, a violation of 18 U.S.C. § 1349 (Count One). (See Docket #12 (criminal indictment).) The government also charged Mr. Nestor with one count of Fraud in Connection with Computers, a violation of 18 U.S.C. § 1030(a)(4) (Count Three). Count Three alleges Mr. Nestor violated § 1030(a)(4) by knowingly and with the intent to defraud access a protected computer in a manner that "exceed[ed] his authorized access." The facts pertaining to Count Three are as follows.

From on or about April 2009 to on or about September 2009, the government alleges Mr. Nestor and Mr. Kane engaged in a conspiracy to obtain money by defrauding gaming machines at casinos in Las Vegas, Nevada and Pennsylvania. The alleged fraudulent act involved exploiting a programming glitch on certain multi-game video poker machines manufactured by International Gaming Technologies, Inc. (IGT).

The government alleges Mr. Kane and Mr. Nestor illegally took advantage of the glitch in the video poker machines in the following manner:

1. Mr. Kane and Mr. Nestor would ask an attendant to activate the "double up" feature on certain IGT multi-game video poker machines.
2. After the attendant activated the "double up" feature, Mr. Kane and Mr. Nestor would play a randomly selected game until they won a hand.
3. After winning a hand, they would then exit the game and select a different poker game.
4. Again, they would play till they won another hand.
5. They would then insert either currency or a cash voucher into the machine.
6. They would then exit the game, and select a higher gambling denomination (e.g., if they were originally playing $1 per hand, they would switch to $20)
7. They would then select the original game they played on the machine (see step 2)

8. They would then cash out. Because of a series of programming errors, the machine re-evaluated the original game at the new, higher denomination.

(See Exhibit A (FBI 302 prepared by SA Bugni); see also Exhibit B (video demonstration of exploit made by Nevada Gaming Control Board).)

The government alleges that Mr. Kane and Mr. Nestor performed this exploit at casinos throughout the Las Vegas area, including the Silverton Casino Lodge, the Fremont, the Golden Nugget, the Orleans, the Texas Station, the Fremont, Harrah's, the Rio, and the Wynn. Mr. Nestor also allegedly performed this exploit at the Meadow Casino in Washington County, Pennsylvania.

II.

ARGUMENT

The instant case presents an issue which no court has had occasion to address: Does a person "exceed his authorized access" to a "protected computer" in violation of 18 U.S.C. § 1030(a)(4) when he knows of a programming flaw in a gaming machine that is not connected to the internet, the machine provider gives him access to a game setting which permits him to exploit the programming flaw, and uses that access to obtain money?

Mr. Nestor asserts these actions did not violate § 1030(a)(4). As will be described below, the gaming machines used in the alleged criminal activity are not "protected computers" as contemplated by 18 U.S.C. § 1030. Additionally, Mr. Nestor did not exceed his authorized access to the gaming machines as defined by 18 U.S.C. § 1030(e)(6) because he was freely given access to the "double up" feature on the gaming machines by the casino attendants, and then merely played the games as they were created.

Moreover, dismissal is appropriate in this case because § 1030(a)(4) is unconstitutionally vague. Because courts across the country have reached divergent conclusions about what the terms "access" and "exceeds authorized access" mean, the statute is not "sufficiently definite to give notice of the required conduct to one who would avoid its penalties, and to guide the judge in its application and the lawyer in defending one charged with its violation." Boyce Motor Lines v. United States, 342 U.S. 337, 340 (1952). Accordingly, Count Three must be dismissed.

A. Mr. Nestor's Actions Do Not Constitute a Violation of the Computer Fraud and Abuse Act Because: (1) the Gaming Machines Are Not "Protected Computers," and (2) Mr. Nestor Did Not "Access" or "Exceed his Authorized Access" to the Machines.

1. 18 U.S.C. § 1030 – The Computer Fraud and Abuse Act

Congress enacted the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, in 1984 to enhance the government's ability to prosecute computer crimes. Initially, the act was "designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to 'access and control high technology processes vital to our everyday lives....'" LVRC Holdings v. Brekka, 581 F.3d 1127, 1130-31 (9th Cir. 2009) (quoting H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 1984)); see also Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 1561, 1563-64 (2010); Michael Hatcher, et al., Computer Crimes, 36 Am. Crim. L. Rev. 397, 402 (1999). Gradually, however, the CFAA has been expanded to encompass virtually any manner of computer crime. The majority of crimes targeted by the CFAA involve accessing computers without authorization or in excess of authorization, and then taking specific forbidden actions. See 18 U.S.C. § 1030(a)(1)–(7) (2008).

Pursuant to § 1030(a)(4), the statute at issue here, it is unlawful for a person to

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

18 U.S.C. § 1030(a)(4) (2008).

In order to obtain a conviction under § 1030(a)(4), the government must prove that Mr. Nestor (1) accessed a "protected computer;" (2) exceeding authorization that was granted; (3) knowingly and with intent to defraud and thereby; (4) furthered the intended fraud and obtained anything of value; causing (5) "a loss to one or more persons during any one-year period aggregating at least $5,000 in value." Brekka, 581 F.3d at 1133 (citing P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore LLC, 428 F.3d 504, 508 (3d. Cir. 2005) and Theofel v. Farley-Jones, 359 F.3d 1066, 1078 (9th Cir. 2004)). Only the first two elements—whether Mr. Nestor accessed

a "protected computer" in a manner that exceeded his authorized access—are relevant to the instant motion.

2. Mr. Nestor Did Not Access a "Protected Computer"

Arguably, the gaming machines utilized in the alleged offense qualify as "computers" under § 1030(e)(1). The CFAA defines a computer as

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

18 U.S.C. § 1030(e)(1). According to IGT, the gaming machines it manufactures all contain a processor board which regulates all game functions, including coin acceptance and delivery, game statistical data accumulation and accounting, and player panel switches. See Introduction to Slots and Video Gaming at 14.[1] Because the processor boards perform complex logical and storage functions, the gaming machines are probably "computers" for the purposes of the CFAA. They are not, however, "protected computers."

In pertinent part, the CFAA defines a "protected computer" as a computer

> which is used in or affecting interstate commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications of the United States.

18 U.S.C. § 1030(e)(2)(B).

The gaming machines here are not "protected computers" under this definition because they are not "used in or affecting interstate commerce." Courts which have addressed whether a specific computer qualifies as a "protected computer" have uniformly agreed that a connection to the internet is sufficient to establish a computer was used in interstate commerce and is therefore a "protected computer." See United States v. Fowler, 2010 WL 4269618 at *2 (M.D. Fla. Oct. 25, 2010) (trial evidence that computers were connected to the internet sufficient to establish use in interstate commerce); see also Multiven, Inc. v. Cisco Systems, Inc.,725 F.Supp. 2d 887, 891-

[1]Available online at http://media.igt.com/Marketing/PromotionalLiterature/IntroductionTo Gaming.pdf

92 (N.D.Cal. 2010) (finding that a computer connected to the internet was a protected computer); National City Bank, N.A. v. Prime Lending, Inc., 2010 WL 2854247 at *4 n.2 (E.D.Wash. July 19, 2010) (stating that "any computer connected to the internet is a protected computer"); Expert Janitorial, LLC v. Williams, 2010 WL 908740 at *8 (E.D.Tenn. Mar.12, 2010); Dedalus Foundation v. Banach, 2009 WL 3398595, at *2 (S.D.N.Y. Oct.16, 2009) (unreported) (noting that courts have "found that computers that access the Internet through programs such as email qualify as protected computers"); Continental Group, Inc. v. KW Property Management, LLC, 622 F.Supp.2d 1357, 1370 (S.D.Fla.2009) (noting that a connection to the internet affects interstate commerce or communication); United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (finding that computers connected to the internet "were part of a system that is inexorably intertwined with interstate commerce); accord United States v. Drew, 259 F.R.D. 449, 457-58 (C.D. Cal., 2009); U.S. v. Walters, 182 Fed. Appx. 944, 945 (11th Cir.2006) (stating that the internet is an instrumentality of interstate commerce).

Here, the government has produced no evidence the gaming machines accessed by Mr. Nestor are connected to the internet or a network which uses interstate channels of communications. Thus, at least under the above authority, the gaming machines do not appear to be protected computers.

The CFAA is written broadly enough that it covers computers that are not connected to the internet, so long as those computers are used to conduct business across state lines. See Patrick Patterson Custom Homes, Inc. v. Bach, 586 F.Supp.2d 1026, 1033-34 (N.D.Ill.2008). ("[I]t suffices to state the computer was used for the business and the business operated in two different states."); see also Kerr, supra, Vagueness Challenges at 1570-71 (noting that the CFAA applies to all computers "so long as the federal government has the power to regulate them"). However, the government has produced no evidence that the gaming machines are used in a manner which affects interstate commerce. The gaming machines here were manufactured by a Nevada-based company, are owned and operated by various Nevada-based gaming companies, and are regulated by a state entity—the Nevada Gaming Control Board. Although this is probably a trial issue, there is no

indication that the strictly intrastate use and regulation of the gaming machines are used in interstate commerce. Thus, they are not "protected computers" under the CFAA.

3. Mr. Nestor Did Not Exceed His Authorized Access to the Gaming Machines

The government has also failed to demonstrate Mr. Nestor exceeded his authorized access to the gaming machines in violation of the CFAA. As described above, the government alleges Mr. Nestor violated § 1030(a)(4) by asking casino attendants to activate the "double up" feature on certain models of IGT gaming machines, then performed a series of steps that exploited a flaw in the machines' programming to trigger a jackpot which paid out at a higher denomination than Mr. Nestor had initially wagered. Although Mr. Nestor's alleged actions may have violated Nevada state law,[2] these actions did not exceed his authorized access to the gaming machine in violation of the CFAA.

a. The Various Definitions of "Access"

The CFAA does not define "access." Instead, it has been left to the courts to determine what that word means in the context of the CFAA. This has resulted in a variety of conclusions about what that term means. Under some definitions, a user only "accesses" a computer when she is granted access "inside" the computer to manipulate information and processes. See Orrin Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1624-28 (2003) (citing State v. Allen, 917 P.2d 848 (Kan. 1996) and Moulton v. VC3, 2000 WL 33310901 (N.D. Ga., 2000). Other courts have formulated broader definitions, finding that "access" refers to mere physical "access" to a computer—for example, sending an email to a computer. See id. at 1626-28 (comparing cases).[3]

/ / /

/ / /

---

[2] See, e.g., Nev. Rev. Stat. § 465.070(3) (West 2011) (making it a crime to "claim, collect or take...anything of value from a gambling game with the intent to defraud, without having made a wager contingent thereon, or claim...an amount greater than the amount won").

[3] As will be discussed below, the lack of consensus regarding the definition of "access" supports Mr. Nestor's assertion that § 1030 is unconstitutionally vague.

b. The Various Definitions of "Exceeds Authorized Access"

The CFAA defines "exceeds authorized access" as "access[ing] a computer with authorization and us[ing] such access to obtain or alter information in the computer that the accesser is not entitled to so obtain or alter." 18 U.S.C. § 1030(e)(6). Courts analyzing this definition have taken a number of different approaches in their analysis. See generally, Orin Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1628-40 (2003); see also Orbit One Communications, Inc. v. Numerex Corp., 692 F.Supp. 2d 373, 385 & nn.65 and 66 (S.D.N.Y. 2010) (compiling various approaches to interpreting § 1030(e)(6)).

In the Ninth Circuit, there are currently two conflicting interpretations of "exceeds authorized access."[4] The first definition appears in LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009), which considered the construction of the phrase "without authorization" in § 1030(a)(4). There, the Circuit held that "a person who 'exceeds authorized access,'... has permission to access the computer, but accesses information on the computer that the person is not entitled to access." Brekka, 581 F.3d at 1133.

Thus, applying Brekka in the criminal context, a person may have access to the website of a financial institution such as Bank of America because she has an account with that institution. Pursuant to the terms of a user agreement, she is authorized to access the Bank of America website to monitor her account, make deposits, and transfer money. In other words, she is only entitled to access information about her own account. The user will exceed her authorized access if she begins accessing other users' accounts to gather information about their finances or transfer their money into her own account.

More recently, the Ninth Circuit altered its holding in Brekka. In United States v. Nosal, 642 F.3d 781 (9th Cir. 2011), the defendant was an employee at Korn/Ferry, an executive search firm. When Nosal and all other employees logged into Korn/Ferry's database, the computer

[4] Although the CFAA was designed to target computer hackers, most of the case law interpreting its provisions, including the two leading cases from the Ninth Circuit, arise in the context of employer/employee disputes.

system displayed a notification which stated:

> This computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and *to do so without the relevant authority can lead to disciplinary action or criminal prosecution*.

Id. at 783 (emphasis in original). After Nosal left Korn/Ferry, he solicited three Korn/Ferry employees to work for him. Id. Those three employees then obtained trade secrets by transferring source lists, names, and contact information from Korn/Ferry's database to Nosal. Id.

In finding that Nosal violated the CFAA, the Circuit formulated a broader interpretation of "exceeds authorized access." According to the Nosal panel, "the only logical interpretation of 'exceeds authorized access' is that the employer has placed limitations on the employee's 'permission to use' the computer and the employee has violated—or 'exceeded'—those limitations." Id. at 787. Unlike Brekka, the Nosal opinion seems to indicate that the mere act of going beyond the scope of access as proscribed by an employer violates § 1030, regardless of whether the employee exceeds her access for the purpose of obtaining information to which she is not entitled. Thus, under the Nosal definition of "unauthorized access," a violation of § 1030 might occur under the following circumstances: a federal court employee, as part of her employment, is required to use an office-issued computer to perform certain tasks like performing legal research. If the employee uses that computer for some other purposes, such as visiting social networking sites or checking her personal email account, that employee is potential committing a federal offense under the CFAA.

c. Mr. Nestor Did Not Violate the CFAA Under Either the Brekka or Nosal Definition of "Exceeds Authorized Access"

Regardless of which definition this Court chooses to apply, Mr. Nestor did not violate § 1030(a)(4) by exceeding his authorized access to the gaming machine.[5] As an initial matter, Mr. Nestor did not "access" the gaming machine. As the government's indictment alleges, Mr. Nestor would ask a casino attendant to activate the "double up" feature on the gaming machines, and then

[5] As with the judicial conflicts regarding "access," the tension between these two definitions of "exceeds authorized access" support's Mr. Nestor's argument that § 1030 is unconstitutionally vague.

would place wagers in a manner consistent with the machine's user interface. There is no evidence Mr. Nestor accessed or manipulated the information contained within the gaming machines' processor—he was simply gambling in a way which was allowed by the machine.

Conceivably, Mr. Nestor might have "accessed" the computer if he had discovered a way to manipulate the machines so that he was able to view information normally available only to machine attendants or activate the "double up" feature, or used some external device to manipulate the machines' internal processes. The government has made no such allegation. Moreover, it appears the only people who ever "accessed" the machines were the casino attendants who activated the "double up" feature. Thus, the government has failed to allege Mr. Nestor "accessed" the machines.

Even assuming Mr. Nestor "accessed" the machines, the government has failed to allege Mr. Nestor "exceeded" his authorized access under either the Brekka or Nosal formulation of the term. Applying the Brekka standard to the facts alleged by the government, Mr. Nestor did not exceed his authorized access to the gaming machines because he did not "access information he was not entitled to access." Instead, as noted above, the casino attendants activated a special game feature on the gaming machine, and Mr. Nestor played the games in a manner designed to ensure a high payout. Knowing that a machine has a programming flaw, and pressing buttons in a manner designed to exploit that flaw, is not equivalent to "accessing" information he was not entitled to under Brekka.

The government's allegations also fail to rise to the level of "exceeding authorized access" under Nosal. Unlike Nosal, there is no evidence here that users of the gaming machines were greeted with some sort of use disclaimer outlining the limitations on how they may use the gaming machines when they sit down to play. More importantly, as noted repeatedly, the people in control of the machines—the casino attendants—gave Mr. Nestor access to the "double up" feature. Thus, any plays made during his granted access to the feature did not violate any limitations on his play. Accordingly, Count Three of the indictment must be dismissed.

/ / /

B. 18 U.S.C. § 1030 is Unconstitutionally Vague

When construing a statute, a court ordinarily first looks to the plain meaning of the language in question. See United States v. Hurt, 795 F.2d 765, 770 (9th Cir. 1986), as amended, 808 F.2d 707 (9th Cir. 1987). Given the competing definitions of "access" and "exceeds authorized access" described above, § 1030 is unconstitutionally vague.

The vagueness doctrine "requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." Kolender v. Lawson, 461 U.S. 352, 357 (1983) (internal citations omitted); see also Boyce Motor Lines v. United States, 342 U.S. 337, 340 (1952) ("A criminal statute must be sufficiently definite to give notice of the required conduct to one who would avoid its penalties, and to guide the judge in its application and the lawyer in defending one charged with its violation."); Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498 (1982) ("[W]e insist that laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly").

A statute is unconstitutionally vague if it "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." United States v. Williams, 553 U.S. 285, 304 (2008)(citations omitted); accord United States v. Kilbride, 584 F.3d 1240, 1257 (9th Cir. 2009).

The vagueness doctrine also reinforces fundamental notions concerning the control of the discretion of law enforcement:

> Although the doctrine focuses both on actual notice to citizens and arbitrary enforcement, we have recognized recently that the more important aspect of vagueness doctrine "is not actual notice, but the other principal element of the doctrine-the requirement that a legislature establish minimal guidelines to govern law enforcement."

Kolender, 461 U.S. at 357-58 (citing Smith v. Goguen, 415 U.S. 566, 574 (1974)), accord City of Chicago v. Morales, 527 U.S. 41, 60 (1999)(plurality).

"What renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved; but rather the indeterminacy of precisely what the fact is." Williams, 553 U.S. at 306 (citations omitted); accord

United States v. Schales, 546 F.3d 965, 973 (9th Cir. 2008). Here, the competing interpretations of "access" and "exceeds authorized access" demonstrates there is indeterminancy regarding what acts violate the statute.[6]

III.

CONCLUSION

Based upon the above and foregoing, Mr. Nestor respectfully requests this Court enter an order dismissing Count Three of the Indictment.

Respectfully submitted:

/s/ Shari Kaufman

By:_____
SHARI L. KAUFMAN
Assistant Federal Public Defender

[6] The Ninth Circuit may agree that the definition of "exceeds authorized access" has not been satisfactorily addressed in either Brekka or Nosal. On October 27, 2011, the Circuit issued an order that the case be reheard en banc. See United States v. Nosal, CA No. 10-10038 (9th Cir. Oct. 27, 2011) (Order).

CERTIFICATE OF ELECTRONIC SERVICE

The undersigned hereby certifies that she is an employee of the Law Offices of the Federal Public Defender for the District of Nevada and is a person of such age and discretion as to be competent to serve papers.

That on November 9, 2011 she served an electronic copy of the above and foregoing **MOTION TO DISMISS COUNT THREE OF THE INDICTMENT FOR FAILURE TO STATE AN OFFENSE AND VAGUENESS (Oral Argument Requested)**, by electronic service (ECF) to the person named below:

DANIEL G. BOGDEN
United States Attorney
MICHAEL CHU
Assistant United States Attorney
333 Las Vegas Blvd. So., 5th Floor
Las Vegas, Nevada 89101

/s/ Bonnie S. Bell
_____
Employee of the Federal Public Defender